대 한 민 국 특 허 청
KOREAN INTELLECTUAL PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Intellectual Property Office.

출 원 번 호 : 특허출원 2002년 제 3877 호
Application Number PATENT-2002-0003877

출 원 년 월 일 : 2002년 01월 23일
Date of Application JAN 23, 2002

출 원 인 : 월드탑텍(주)
Applicant(s) WORLD TOPTEC CO., LTD.

2002 년 02 월 07 일

특 허 청
COMMISSIONER

CERTIFIED COPY OF
PRIORITY DOCUMENT

【서지사항】

【서류명】	특허출원서
【권리구분】	특허
【수신처】	특허청장
【제출일자】	2002.01.23
【발명의 명칭】	정보 암호화 방법
【발명의 영문명칭】	METHOD FOR CRYPTOGRAPHING A INFORMATION
【출원인】	
【명칭】	월드탑텍 (주)
【출원인코드】	1-2001-019981-5
【대리인】	
【명칭】	특허법인 엘엔케이
【대리인코드】	9-2000-100002-5
【지정된변리사】	변리사 이헌수
【포괄위임등록번호】	2001-028097-6
【발명자】	
【성명의 국문표기】	이동향
【성명의 영문표기】	LEE,DONG HYANG
【주민등록번호】	591228-1009518
【우편번호】	406-050
【주소】	인천광역시 연수구 옥련동 럭키아파트 107동 1103호
【국적】	KR
【우선권주장】	
【출원국명】	KR
【출원종류】	특허
【출원번호】	10-2001-0030164
【출원일자】	2001.05.30
【증명서류】	첨부
【심사청구】	청구
【조기공개】	신청
【취지】	특허법 제42조의 규정에 의하여 위와 같이 출원합니다. 대리인 특허법인 엘엔케이 (인)

【수수료】

【기본출원료】	20	면	29,000 원
【가산출원료】	9	면	9,000 원
【우선권주장료】	1	건	26,000 원
【심사청구료】	8	항	365,000 원
【합계】	429,000 원		
【감면사유】	소기업 (70%감면)		
【감면후 수수료】	146,900 원		

【첨부서류】 1. 소기업임을 증명하는 서류_1통

【요약서】

【요약】

본 발명은 유,무선 망을 기반으로 하는 컴퓨터에서 실행 가능한 정보 암호화 방법에 관한 것으로, 정보 암호화를 위한 공개키와 암호개인키를 생성하는 단계와; 생성된 공개키와 암호화 실행 모듈을 클라이언트 단말기로 전송하는 단계와; 클라이언트 단말기에서 상기 공개키와 암호화 실행 모듈이 실행되어 암호화된 정보를 상기 클라이언트 단말기로부터 수신하는 단계와; 상기 암호개인키를 추출하여 수신한 암호화된 정보를 복호화하는 단계;를 포함하는 것을 특징으로 한다.

【대표도】

도 2

【색인어】

암호화, 인증, 결제.

【명세서】

【발명의 명칭】

정보 암호화 방법{METHOD FOR CRYPTOGRAPHING A INFORMATION}

【도면의 간단한 설명】

도 1은 본 발명의 실시예에 따른 시스템 구성도.

도 2는 본 발명의 일실시예에 따른 사용자 인증 암호화 처리 흐름도.

도 3은 도 2중 공개키 생성을 위한 암호화 모듈 구동 절차 흐름도.

도 4는 도 2중 클라이언트 단말기(100)에서 실행되는 사용자 정보 암호화 및 메시지 축약과정을 설명하기 위한 절차 흐름도.

도 5는 도 2중 웹 인증서버(200)에서 실행되는 사용자 정보 복호화 과정을 설명하기 위한 절차 흐름도.

도 6은 본 발명의 일실시예에 따른 사용자 인증정보 암호화 방법을 이용하여 결제 수행하는 결제시스템 서버(300)의 절차 흐름도.

도 7은 본 발명의 일실시예에 따른 사용자 인증을 위한 정보 암호화 방법이 무선망 시스템에서 사용되는 실시예를 설명하기 위한 도면.

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

<8> 본 발명은 전송 정보의 암호화 시스템에 관한 것으로, 특히 웹상에서 클라이언트가 입력한 정보를 암호화하여 전송하는 논-인스톨(non-install) 방식의 정보 암호화 방법에 관한 것이다.

<9> 일반 웹 사이트에서 사용자 인증방법으로 가장 널리 사용되는 것이 로그인(Login)방식이다. 이는 사용자 ID와 패스워드를 데이터로 하여 사용자에 대한 적합성 여부를 판단하는 방법으로서 구현이 쉽고 관리가 용이하기 때문에 가장 기본적인 사용자 인증방법으로 자리매김하고 있다.

<10> 그러나 일반적인 로그인 방식은 로그인 정보에 대하여 전송과정에서 악의적인 제3자에 의해 절취되거나 왜곡될 소지가 높다. 이를 막기 위해 인증 및 암호화 개념이 도입되기에 이르렀으며, 현재 가장 대표적으로 사용되는 방식은 클라이언트 컴퓨터에 인증을 위한 개인정보와 이 개인이 인증받았음을 증명하는 인증서, 자료 교환을 위한 핑거 프린트(finger print)라 일컫는 암호화키가 저장되어 있는 인증서를 인스톨시키는 방법이다.

<11> 인증서 배포방식은 네트워크 통신에 있어 소켓 단계에서 암호화되어 송수신하는 SSL(Secure Sockets Layer)과 결합되어 활용되고 있으며, 근간에는 보안통신의 표준으로 자리잡고 있다. e-biz와 관련된 거의 모든 결제시스템에서 채택하고 있는 SSL은

<12> - 클라이언트와 서버 사이의 상호인증(공개키 방식:RSA-1024비트)

<13> - 클라이언트 컴퓨터 메시지 축약(MD-5 혹은 SHA-1등), 암호화(대칭키 방식:DES 혹은 RC5 등)되어 저장되어 있는 사용자정보의 전송단계를 거치며, 교환되는 자료형식은 국제적 표준형식(ITU의 X.509)으로 지정되어 있다.

<14> 국제적 공인방식으로 안전성에 상당한 신뢰감을 확보하여 일반화된 SSL은 데이터 처리과정에서 인증을 위해 여러 가지의 단계, 예를 들면 공개키 방식을 이용한 대칭키 교환(handshake과정), 메시지 축약, 대칭키로 암호화되어 있는 자료의 전송단계를 거치는데, 특히 핸드쉐이크 과정이라 일컫는 공개키 방식을 이용한 대칭키 교환과정의 경우에는 서버에 가해지는 부담이 실로 막대하다 할 것이다. 또한 사용자 각각이 전송해야 할 인증자료의 크기만도 2K바이트에 달하며, 이 외에도 인증자료 컴파일을 위한 별개의 모듈을 갖추어야 하는 등, 인증서버에 가해지는 부담이 큰 단점이 있다. 이러한 이유로 서버성능은 저하되고 데이터 처리속도 및 네트워킹 속도가 SSL 서비스를 제공하지 않는 서버에 비해 다소 떨어진다. 또한 웹 서버 외에 SSL 서비스시 사용되는 인증서들의 관리를 위해 고가의 인증서 관리 시스템을 부가적으로 구축해야 하기 때문에, SSL 서버구축에 따른 추가적인 인력 및 비용이 발생하며, 이로 인한 업무부담이 가중되는 문제가 발생하게 된다.

<15> 내부 알고리즘적인 측면에서도 SSL이 키교환시 사용하고 있는 표준 알고리즘인 RSA의 경우 안정성 확보를 위해 최소 키크기가 1024비트로 타원 곡선 암호화(Elliptic Curve Cryptography:ECC)의 160비트에 비해 월등히 커, 보안수준 조정시 서버에 가해지는 부담과 전송용량에 커다란 부담을 안겨 주는 단점이 있다.

<16> 또한 SSL의 인증서 발급 방식은 클라이언트 컴퓨터에 인스톨되어야만 한다는 단점을 갖고 있다. 이러한 시스템은 인증서의 중복발급을 불허하고 있어 사용자가 컴퓨터를 옮겨 다니며 인증서버에 접속하는 경우 기존의 인증서를 폐기하고 항상 새로운 인증서를 다운받아야 하는 불편함이 있다. 더욱이 기존의 인증서 방식은 인증서버에 따라 각각 개별적인 인증서를 발급하기 때문에, 특정 웹 페이지를 이용하기 위해서는 그 웹 페이지에서 허용하는 인증서를 받아야만 하므로 인증장치의 범용성이 다소 떨어지는 단점이 있다.

<17> 이러한 단점은 디바이스(device)상의 가용한 자원(resource)이 빈약하고, 네트워크 자체 성능이 상대적으로 떨어지는 무선환경에 있어 더욱 큰 문제점으로 부각된다. 왜냐하면 무선환경에서 SSL과 같은 구동방식으로 작동하는 WTLS나 SSL의 경우, 네트워크 구조상 트랜스포트 레이어(Transport Layer)에서 프로토콜적으로 작동하기 때문에 보안을 요구하는 정보가 게이트웨이를 통과할 때 프로토콜 변환에 의해 보안상의 공백이 발생하여 '종단간 보안(End to End)' 확보가 어렵기 때문이다. 또한 무선환경에서는 보안활동이 일원화되어 있지 못하기 때문에 이의 관리 및 운용상 부하가 커짐에 따라 서버의 부담이 가중되는 한편, 네트워크 성능이 저하되는 문제를 수반하게 된다.

<18> 한편 인증서 기반의 SSL 등에 비해 비교적 사용절차가 단순한 SSH(Secure SHell)의 경우에 있어서도 웹에 이식되는 방식이 아닌 인스톨 방식으로 사용하게 되어 있어, 초기화에 어려움이 있고 웹 이식시 번거로움이 따라 일반적으로 사용되지 않고 있다.

【발명이 이루고자 하는 기술적 과제】

<19> 따라서 본 발명의 목적은 유,무선 네트워크 통신시 클라이언트 단말기에 사용자 인증을 위한 인증서의 설치 없이도 사용자 인증이 가능한 논-인스톨(non-install)방식의 정보 암호화 방법을 제공함에 있다.

<20> 본 발명의 또 다른 목적은 클라이언트로부터 웹 서버로 전송되는 암호화 데이터의 용량을 줄임으로서 데이터 처리 속도 및 네트워킹 속도를 향상시킬 수 있는 정보 암호화 방법을 제공함에 있다.

<21> 본 발명의 또 다른 목적은 암호화된 정보 처리를 위한 서버의 부담을 경감시켜 줄 수 있는 정보 암호화 방법을 제공함에 있다.

<22> 본 발명의 또 다른 목적은 웹 브라우져나 서버에 관계없이 각종 버츄얼 머신 플랫폼이나 OS상에서 수행될 수 있는 하나의 응용 프로그램으로서의 정보 암호화 방법을 제공함에 있다.

【발명의 구성 및 작용】

<23> 상기 목적을 달성하기 위한 본 발명의 일 양상에 따른 정보 암호화 방법은;

<24> 정보 암호화를 위한 공개키와 암호개인키를 생성하는 단계와;

<25> 생성된 공개키와 암호화 실행 모듈을 클라이언트 단말기로 전송하는 단계와;

<26> 클라이언트 단말기에서 상기 공개키와 암호화 실행 모듈이 실행되어 암호화된 정보를 상기 클라이언트 단말기로부터 수신하는 단계와;

<27> 상기 암호개인키를 추출하여 수신한 암호화된 정보를 복호화하는 단계;를 포함하는 것을 특징으로 한다.

<28> 이하 본 발명의 바람직한 실시예를 첨부 도면을 참조하여 상세히 설명하기로 한다. 본 발명을 설명함에 있어, 타원 곡선 암호화 알고리즘과 같이 이미 공지된 기능 혹은 구성에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우 그에 대한 상세한 설명은 생략하기로 한다. 그리고 하기 설명에서는 사용자 인증 정보와 결제정보를 예로 들어 본 발명의 바람직한 실시예에 따른 정보 암호화 방법을 설명하기로 한다.

<29> 우선 도 1은 본 발명의 실시예에 따른 시스템 구성도를 도시한 것으로, 클라이언트 단말기(100)는 인터넷(150)을 통해 웹 인증 서버(200) 및 서비스 서버(250), 그리고 결제 시스템 서버(300)와 접속 가능하다. 상기 웹 인증 서버(200)는 사용자를 인증하기 위한 실시예를 설명하기 위해 붙여진 명칭으로, 암호화 및 복호화를 전반적으로 수행하는 암호화 서버로 명명될 수도 있다.

<30> 상기 웹 인증 서버(200)는 우선 사용자 정보 DB를 구비하고 있으며, 클라이언트 단말기(100)로부터 접속요구가 있는 경우 암호화 모듈에 의해 생성된 공개키와 메시지 축약모듈(SHA-1) 및 데이터 압축모듈이 포함된 암호화 실행 모듈을 탑재한 로그인 화면을 클라이언트 단말기(100)에 제공한다. 그리고 웹 인증 서버(200)는 상기 암호화 실행 모듈에 의해 암호화, 메시지 축약 및 데이터 압축된 사용자 정보를 전송받아 이를 축약 해제함과 아울러 복호화한후 미리 저장된 사용자 정보와 비교하여 사용자 인증을 수행한다.

<31> 한편 서비스 서버(250)는 사용자 인증완료된 클라이언트가 요구하는 서비스 정보를 제공한다. 이러한 서비스 서버의 예로서 쇼핑 몰을 들 수 있다. 결제 시스템 서버(300) 역시 VAN 혹은 전용전산망을 통해 금융결제기관 서버(350)와 접속가능하며, 서비스 서버(250)의 중재에 의해 접속된 클라이언트 단말기(100)로 암호화 모듈에 의해 생성된 공개키와 메시지 축약 및 데이터 압축 모듈이 포함된 암호화 실행모듈을 탑재한 결제 웹 페이지를 제공한다. 그리고 결제 시스템 서버(300)는 상기 암호화 실행 모듈에 의해 암호화 및 데이터 압축된 카드번호 및 비밀번호와 같은 결제정보를 전송받아 이를 압축 해제함과 아울러 복호화한후 금융결제기관(350) 서버로 전송한다. 이러한 결제정보의 전송 이후 금융결제기관(350) 서버로부터 결제승인결과 정보를 수신하고 이를 클라이언트 단말기(100)에 전송하여 줌으로서, 클라이언트는 결제 승인 및 결제 불가정보를 수신받을 수 있다.

<32> 이하 상술한 구성을 가지는 시스템에서 사용자 인증 암호화가 어떠한 방식으로 수행되며, 이러한 사용자 인증 암호화가 결제시스템에 어떻게 응용되는지를 설명하기로 한다.

<33> 도 2는 본 발명의 실시예에 따른 사용자 인증을 위한 정보 암호화 처리 흐름도를 도시한 것이며, 도 3은 도 2중 공개키 생성을 위한 암호화 모듈 구동 절차 흐름도를, 도 4는 도 2중 클라이언트 단말기(100)에서 실행되는 사용자 정보 암호화과정을 설명하기 위한 절차 흐름도를 도시한 것이다. 그리고 도 5는 도 2중 웹 인증서버(200)에서 실행되는 사용자 정보 복호화 과정을 설명하기 위한 절차 흐름도를 도시한 것이다.

<34> 참고적으로 도 2에 기재된 짝수 참조번호는 웹 인증 서버(200)에서 수행되는 단계를 나타낸 것이며, 홀수 참조번호는 클라이언트 단말기(100)에서 수행되는 단계들을 나타낸 것이다. 도 2를 참조하면, 우선 클라이언트 단말기(100)가 웹 인증 서버(200)에 접속 요청(400단계)하면, 웹 인증 서버(200)는 상기 클라이언트의 접속요청을 이벤트로 하여 암호화 모듈을 구동(402단계)시켜 공개키를 생성한다. 상기 암호화 모듈은 도 3에 도시한 바와 같이 우선 클라이언트의 접속요청이 있을 경우 랜덤한 160비트 암호개인키를 생성(500단계)하여 키관리 DB에 저장(502단계)하고, 이후 암호개인키값과 타원곡선 초기화값에 의해 타원곡선 위의 한 점 좌표를 연산(504단계)함으로서 사용자에게 전송할 공개키값을 생성(506단계)한다. 그리고 생성된 공개키와 무결성 검증을 위한 메시지 축약모듈과 전송량 감소를 위한 데이터 압축모듈이 포함된 암호화 실행모듈을 HTML 파일로 변환(508단계)한후 메인 루틴으로 리턴한다. 즉, 웹 인증 서버(200)는 402단계에서 타원 곡선 암호화(ECC)알고리즘에 기초하여 사용자 정보를 암호화하기 위한 공개키를 생성한다.

<35> 참고적으로 본 발명의 실시예에서는 메시지 축약방법을 무결성 검증을 위한 수단으로 사용하고 있다. 이러한 무결성 검증은 전송된 자료가 전송도중 아무런 왜곡(노이즈에 의하거나, 악의적인 제3자에 의해 변경 혹은 손실되는 것)도 되지 않았다는 것을 확인하기 위한 과정으로서, 먼저 원문을 MD5나 SHA1 알고리즘을 이용하여 메시지축약(Message Digest)을 하여 나온 소정 크기의 결과문을 원문과 함께 서버에 전송하면, 서버측에서는 다시 전송받은 원문을 클라이언트에서와 같은 알고리즘으로 MD하고 이 MD문을 전송받은 MD문과 비교함으로서, 전송과정에서

왜곡이 없었음을 입증하는 방식이다. 참고로 MD5 알고리즘의 경우 36비트, SHA1의 경우 40비트로 축약되며, 축약을 풀수 있는 확률은 SHA1 알고리즘이 더욱 어렵기 때문에 보안효과가 MD5 보다 SHA1이 높다할 수 있다. 그리고 본 발명의 실시예에서는 데이터량의 축소와 2중 보안을 위해서 데이터 압축 모듈을 이용하고 있다. 즉, 데이터 압축 모듈에 암호키값을 부여하게 되는데, 상기 암호키값은 암호화에 사용되는 공개키 가운데 일부분(예를 들면 4개의 숫자)을 임의로 선정하여 사용하며, 이 키값 역시 전송시 자신이 추출된 공개키로 암호화됨으로서 전송시의 안전을 확보한다. 이러한 암호키값을 하기에서 암호화 압축키로 정의하였다.

<36> 한편 웹 인증 서버(200)는 404단계에서 상기 암호화 모듈 구동에 의해 생성된 공개키와 메시지 축약모듈(SHA-1알고리즘 사용) 및 데이터 압축모듈로 구성되는 암호화 실행모듈이 탑재된 로그인화면을 클라이언트 단말기(100)에 제공한다. 상기 암호화 실행 모듈은 상기 공개키와 랜덤한 14비트 정수, 입력된 사용자 정보를 타원곡선 연산을 통해 암호화 실행하는 모듈이며, 상기 메시지 축약모듈은 주어진 메시지의 축약을 담당하는 모듈이다. 또한 데이터 압축모듈은 이 두 모듈의 결과를 압축하는데 사용되며, 선택적으로 탑재될 수 있다. 그리고 본 발명에서는 상기한 모듈들은 모두 자바 애플릿 형태로 상기 로그인 화면에 탑재되는 것으로 한다.

<37> 이와 같이 본 발명에서는 기존의 인증서 인스톨 방식과는 달리, 웹 인증 서버(200)에서 암호개인키와 타원곡선 연산을 통해 사용자 정보 암호화를 위한 공

개키를 생성하고, 이 생성된 공개키와 암호화 실행모듈이 로그인 화면인 웹 페이지에 애플릿 형태로 담겨 클라이언트 단말기(100)로 전송되는 것이다.

<38> 한편 클라이언트 단말기(100)에서는 웹 인증 서버(200)에서 제공된 로그인 화면의 사용자 정보 입력 필드에 사용자 정보인 ID와 패스워드를 입력(405단계)하고 확인버튼을 누르면, 탑재된 암호화 실행모듈에 의해 사용자 정보 암호화 및 데이터 압축이 이루어진다(407단계). 이러한 사용자 정보 암호화와 데이터 압축 과정을 좀 더 상세하게 도시한 도 4를 참조하여 설명하면,

<39> 도 4의 600단계에서는 우선 입력된 사용자 정보값을 공개키와 암호화 실행모듈을 이용하여 암호화함으로서 전송 원문을 생성한다. 그리고 602단계에서는 무결성 검증을 위해 상기 메시지 축약모듈을 이용하여 상기 전송 원문을 축약함으로서 메시지 축약문(MD문)을 생성한다. 그리고 전송량 감축과 2중 암호화를 위해 상기 전송 원문과 메시지 축약문을 데이터 압축 모듈을 이용하여 압축(604)한다. 상기 전송 원문과 메시지 축약문을 압축하기 위해서는 우선적으로 상기 공개키중 소정 의 자리수(이하 암호화 압축키라 함)를 랜덤하게 추출한후 이 암호화 압축키를 이용하여 상기 전송 원문과 메시지 축약문을 압축하면 된다. 이후 상기 암호화 압축키를 안전하게 전송하기 위해 암호화 압축키를 상기 전송 원문을 암호화하기 위해 사용했던 공개키로 암호화(606단계)한후 이를 604단계에서 압축된 값과 함께 웹 문서 파일로 반환한후 도 2에 도시한 메인 루틴으로 리턴한다.

<40> 한편 도 2의 407단계에서 암호화 및 압축된 사용자 정보는 이후 409단계에서 웹 인증 서버(200)로 전송된다.

<41> 그러면 웹 인증 서버(200)는 복호화 모듈을 호출 구동하여 압축 전송된 메시지를 복호화(410단계)한다. 이러한 복호화 모듈의 동작을 도 5를 참조하여 설명하면, 우선 복호화 모듈의 700단계에서는 상기 암호화된 암호화 압축키를 복호화하기 위해 암호개인키를 호출하고, 호출된 암호 개인키를 이용하여 상기 암호화된 암호화 압축키를 복호화(702단계)한다. 그리고 704단계에서는 상기 복호화된 암호화 압축키를 이용하여 압축된 전송 원문과 메시지 축약문(전송받은 MD가 됨)을 압축 해제시킨다. 이후 무결성 검증을 위해 압축해제된 전송 원문을 메시지 축약(706단계)(전송 원문 MD가 됨)하여 이를 전송받은 메시지 축약문(전송받은 MD문)과 동일한가를 비교(708단계)한다.

<42> 만약 비교결과 동일하다면, 즉 무결성 검증이 완료되었다면 712단계에서는 미리 호출된 암호개인키로 전송 원문을 복호화한후 임시 DB에 저장(714)하지만, 무결성 검증이 부결되었을 경우에는 에러 메시지 출력(710단계)이 이루어지도록 한다.

<43> 따라서 상술한 복호화 과정에 의해 웹 인증 서버(200)는 412단계에서 사용자 정보 DB에 저장된 내용과 임시 DB에 저장된 복호화 전송원문을 비교하고 사용자 인증 확인이 정상적으로 이루어졌으면 418단계로 진행하여 로그인을 허용하고, 그 반대이면 회원가입을 유도한다. 만약 416단계에서 회원가입이 이루어졌으면 418단계로 진행하여 로그인을 허용한후 서비스 서버(250)를 연결(420단계)하지만, 회원가입을 거부하면 에러메세지를 클라이언트 단말기(100)로 출력(422단계)하여 준다.

<44> 상술한 바와 같이 본 발명은 클라이언트와 서버간에 전송되는 사용자 정보를 암호화함에 있어서, 클라이언트 단말기에 사용자 정보를 암호화하기 위한 알고리즘의 인스톨 없이 암호화 실행모듈이 탑재된 로그인화면만을 전송하여 사용자 정보의 암호화 및 데이터 압축을 수행하기 때문에, 서버 시스템의 변화에 사용자는 아무런 조정 절차없이 웹에 접속할 수 있으며, 또한 프로그램 업그레이드시 사용자는 자신의 컴퓨터에 의존하지 않고 어느 컴퓨터에서나 안전하게 로그인 할 수 있게 되는 것이다.

<45> 상기에서는 본 발명의 일실시예에 따른 사용자 인증을 위한 정보 암호화 방법에 대해서 구체적으로 설명하였다. 이하에서는 결제정보의 암호화 방법에 대하여 설명하기로 한다.

<46> 도 6은 본 발명의 실시예에 따른 결제정보 암호화를 수행하는 결제시스템 서버(300)의 절차 흐름도를 도시한 것이다.

<47> 우선 도 2에 도시한 절차에 의해 사용자 인증이 완료되었다면, 웹 인증 서버(200)는 연결되어 있는 서비스 서버(250)로 클라이언트 단말기(100)를 연결해 주고, 클라이언트가 서비스를 이용하다 결제페이지에 접속하게 되면 서비스 서버(250)는 클라이언트를 결제 시스템 서버(300)로 연결시켜 준다. 혹은 결제 시스템 서버(300) 자체에서 도 2에 도시한 절차에 의해 사용자 인증이 완료되었다면 클라이언트 단말기(100)와 결제 시스템 서버(300)는 접속이 이루어질 것이다. 이와 같이 클라이언트와 접속이 이루어졌다고 판단(800단계)되면 결제 시스템 서버(300)는 802단계로 진행하여 도 2에서 설명한 바와 같이 공개키와 메시지 축

약모듈 및 데이터 압축모듈로 구성되는 암호화 실행모듈이 탑재된 결제 웹 페이지를 클라이언트 단말기(100)에 제공하여 준다.

<48> 그러면 클라이언트는 결제 웹 페이지에 제공된 카드번호 및 비밀번호와 같은 결제정보 입력 필드에 해당정보를 입력하고 확인을 선택하면, 상기 결제정보는 도 2에서 설명한 바와 같이 암호화 실행모듈에 의해 결제정보의 암호화와 축약 및 압축이 이루어져 결제 시스템 서버(300)로 전송된다. 이에 결제 시스템 서버(300)는 암호화 및 압축된 결제정보의 수신이 있는가를 판단(804단계)하여 수신되었으면 806단계로 진행하여 복호화 모듈을 호출 구동시킨다. 상기 복호화 모듈의 구동에 의해 우선적으로 암호화 압축키가 암호개인키에 의해 복호화되고, 복호화된 암호화 압축키에 의해 전송원문이 압축해제되며, 압축해제된 전송원문을 다시 메시지 축약하여 이를 전송받은 메시지 축약문과 비교하여 무결성 검증을 수행한다. 무결성 검증이 성공적으로 이루어졌으면 암호개인키에 의해 전송원문이 복호화된다. 이와 같이 복호화된 결제정보는 이후 금융결제기관(350) 서버로 전송(808단계)됨으로서, 결제 시스템 서버(300)는 이후 상기 금융결제기관(350) 서버로부터 결제승인결과 정보를 수신(810단계)받게 된다. 이와 같이 결제승인결과 정보를 수신받은 결제 시스템 서버(300)는 이후 812단계에서 결제승인결과 정보를 클라이언트 단말기(100)로 전송하여 줌으로서, 클라이언트는 결제승인결과 정보에 따라 결제정보 재 입력, 서비스 제공요청 등과 같은 추후의 동작을 취할 수 있게 되는 것이다.

<49> 따라서 본 발명은 전자상거래시 수반되는 결제방법에 있어서 논-인스톨 방식의 정보 암호화 방법을 도입함으로서 결제정보의 암호화 수준을 높일 수 있게

되는 것이며, 전체적인 암호화 용량이 작아 기존의 SSL방식 보다 속도가 빠르며, 서버에 가해지는 부담 또한 경감시킬 수 있다.

<50> 이상에서는 가장 보편화되어 있는 유선망을 고려하여 본 발명의 실시예에 따른 사용자 인증정보, 결제정보의 암호화 방법을 설명하였으나, 별 다른 변형없이 무선망 시스템에서도 본 발명을 구현할 수 있다. 이에 대하여 보다 구체적으로 설명하면,

<51> 우선 도 7은 본 발명의 실시예에 따른 사용자 인증정보 암호화 방법이 무선망 시스템에서 사용되는 실시예를 설명하기 위한 도면을 도시한 것으로 PDA, 휴대폰과 같은 무선 단말기(370)는 일실시예로 WAP 프로토콜을 통해 G/W(Gateway)(360)와 데이터 송수신이 가능하며, 상기 G/W(360)는 인터넷망(150)을 통해 HTTP 프로토콜에 근거하여 웹 인증 서버(200)와 접속 가능하다. 상기 웹 인증 서버(200)는 도 1에 도시한 웹 인증서버와 동일 기능을 수행하는 서버이며, 도면부호 250, 300, 350 역시 도 1에서 설명한 블럭들과 동일 기능을 수행하므로 그에 대한 상세 설명은 생략하기로 한다.

<52> 일반적인 무선망에서의 무선 인터넷 접속 과정을 설명하면, 무선 단말기(370)는 인터넷에 접속하기 위하여 우선적으로 게이트웨이(360)에 접속되어야 한다. 이러한 경우 무선 단말기(370)와 게이트웨이(360) 사이에는 WTLS(Wireless Transport Layer Security) 프로토콜에 의한 통신이 이루어진다. 그리고 무선 단말기(370)와 접속이 이루어진 게이트웨이(360)는 URL을 검색하여 해당 웹 서버, 예를 들면 웹 인증 서버(200)로 접속요구를 시도하게 되는데, 이러한 경우 게이트웨이(360)와 웹 인증 서버(200) 사이에는 SSL에 의한 통신이 이루어진다.

<53> 따라서 웹 인증 서버(200)에서 무선 단말기(370)로 통신이 이루어지는 경우 혹은 그 반대의 경우에 있어서도, 게이트웨이(360)에서 암호가 순간적으로 풀렸다가 다시 암호화과정이 이루어지기 때문에, 게이트웨이(360)측면에서 보면 암호화문을 평문화하고 이를 다시 암호화하여 전송하여야 하기 때문에 그 만큼 부하가 가중되는 문제가 발생하게 된다. 이는 곧 네트워킹 속도의 저하를 의미함은 물론, 보안상의 허점을 노출시키게 되는 것이다.

<54> 그러나 본 발명의 실시예에 따른 정보 암호화 방법을 사용하게 되면 게이트웨이(360)에서 사용자 단말기로부터 전송된 정보를 평문처리한후 다시 재암호화하여 이를 웹 인증 서버(200)로 전송할 필요가 없기 때문에, 게이트웨이(360)의 부하처리부담 없이 고속 네트워킹이 가능함은 물론, 보안성을 지속적으로 유지시켜 줄 수 있는 효과를 가지게 된다.

<55> 따라서 본 발명은 무선 인터넷 접속 환경에 있어서 보다 강력한 효과를 가진다고 볼 수 있다.

【발명의 효과】

<56> 상술한 바와 같이 본 발명은 논-인스톨 방식의 정보 암호화 방식을 도입함으로서, 암호화 수준 업그레이드에 있어서 사용되는 알고리즘(ECC)의 암호화 단계를 높임으로서 보다 손쉽게 암호화 수준을 높일 수 있는 이점이 있으며, 또한 클라이언트와 서버간에 전송되는 자료를 암호화함은 물론, 암호화시 이용한 키들 중 일부를 다시 암호화 내용 압축시 사용하므로 전송되는 데이터 용량을 감축할 수 있음은 물론, 2중 보안성을 확보할 수 있는 이점이 있다. 그리고 암호화 용량이 작기 때문에 기존의 SSL방식 보다 데이터 처리속도 및 네트워킹 속도가 빠르

며 서버에 가해지는 부담 역시 줄일 수 있는 장점이 있다. 아울러 본 발명은 애플리케이션 레이어(application layer)에서 실행 가능하기 때문에 전송정보의 분석이 가능하며, 이로 인해 중요 정보만을 선별하여 암호화 전송할 수 있기 때문에 모든 정보를 암호화하여 전송하는 기존의 SSL에 비해 서버의 처리 부하를 경감시켜 줄 수 있는 이점이 있다. 아울러 자바 애플릿 혹은 ActiveX 형식을 취함으로서 웹브라우져나 서버에 관계없이 암호화 모듈을 사용할 수 있는 이점이 있으며, 애플릿의 활용으로 구현이 용이한 장점이 있다. 그리고 보안설정을 위한 추가적인 서버구축작업이 필요 없는 효과도 있다.

<57> 또한 인증서를 사용자 컴퓨터에 인스톨하여 사용하는 방식이 아니므로, 프로그램 업그레이드시 사용자는 자신의 컴퓨터에 의존하지 않고 어느 컴퓨터에서나 안전하게 로그인 할 수 있는 장점이 있으며, 인증시스템의 변경에 대해 사용자측에 서버의 용량 증가 등에 따라 부가적으로 가해지는 부담이 없다.

<58> 아울러 본 발명은 서버 시스템의 변화에 사용자는 아무런 조정절차 없이 웹에 접속할 수 있기 때문에 새로 변경된 내용들을 그대로 이용할 수 있는 이점이 있으며, 인증서 관리를 위해 별도의 솔루션을 구입하거나 구축하여야 하는 SSL에 비해 인증서 관리를 위한 부담을 덜 수 있는 효과도 있다.

<59> 그리고 무선 인터넷 접속 환경에서 무선 단말기와 웹 인증 서버간의 통신 수행시 게이트웨이에서 암호화문을 평문화하고 이를 다시 암호화하여 전송할 필요가 없기 때문에, 그 만큼 게이트웨이의 부하처리부담을 경감시켜 줄 수 있을 뿐만 아니라 무선 네트워킹 속도가 향상되는 이점도 있다.

<60> 한편 본 발명은 도면에 도시된 실시예들을 참고로 설명되었으나 이는 예시적인 것에 불과하며, 당해 기술분야에 통상의 지식을 지닌자라면 이로부터 다양한 변형 및 균등한 타실시예가 가능하다는 점을 이해할 것이다. 예를 들면 본 발명의 실시예에서는 사용자 인증을 위한 사용자 정보와 결제를 위한 결제 정보를 암호화하는 것으로 설명하였으나, 이러한 정보들은 결국 암호화하기 위한 전송정보의 예시에 불과하다. 따라서 본 발명의 진정한 기술적 보호범위는 첨부된 특허청구범위에 의해서만 정해져야 할 것이다.

【특허청구범위】

【청구항 1】

네트워크를 통해 클라이언트 단말기와 접속 가능한 서버에서 실행 가능한 정보 암호화 방법에 있어서,

정보 암호화를 위한 공개키와 암호개인키를 생성하는 단계와;

생성된 공개키와 암호화 실행 모듈을 클라이언트 단말기로 전송하는 단계와;

클라이언트 단말기에서 상기 공개키와 암호화 실행 모듈이 실행되어 암호화된 정보를 상기 클라이언트 단말기로부터 수신하는 단계와;

상기 암호개인키를 추출하여 수신한 암호화된 정보를 복호화하는 단계;를 포함하는 것을 특징으로 하는 정보 암호화 방법.

【청구항 2】

청구항 1에 있어서, 상기 암호화된 정보가 로그인시의 사용자 인증정보이고 상기 암호화 방법이;

복호화된 정보를 미리 저장된 정보와 비교하는 정보 인증단계와;

정보 인증결과여부에 따라 클라이언트의 접속을 허가 혹은 차단하는 단계;를 더 포함함을 특징으로 하는 정보 암호화 방법.

【청구항 3】

청구항 1에 있어서, 상기 암호화된 정보가 결제정보이고 상기 암호화 방법이;

복호화된 정보를 접속 가능한 금융결제기관 서버로 전송하는 단계와;

상기 금융결제기관 서버로부터 결제승인결과 정보를 수신하여 상기 클라이언트 단말기로 전송하여 주는 단계;를 더 포함함을 특징으로 하는 정보 암호화 방법.

【청구항 4】

청구항 1 내지 청구항 3중 어느 한 항에 있어서, 상기 공개키는;

생성된 n비트의 암호개인키값과 타원곡선 초기화 값에 의해 타원곡선 위의 한 점 좌표를 연산하여 생성됨을 특징으로 하는 정보 암호화 방법.

【청구항 5】

청구항 1 내지 청구항 3중 어느 한 항에 있어서, 상기 암호화된 정보를 복호화 하는 단계는;

상기 암호개인키를 호출하여 상기 암호화된 정보에 포함된 암호화 압축키를 복호화하는 단계와;

복호화된 상기 암호화 압축키로 상기 암호화된 정보에 포함된 전송 원문과 메시지 축약문을 압축 해제하는 단계와;

압축 해제된 상기 전송원문을 다시 메시지 축약하는 단계와;

메시지 축약된 전송 원문과 압축 해제된 메시지 축약문을 비교하여 동일하면 상기 암호개인키로 압축 해제된 전송 원문을 복호화하는 단계;를 포함함을 특징으로 하는 정보 암호화 방법.

【청구항 6】

무선 단말기들과 통신 수행하는 게이트웨이와 접속 가능한 컴퓨터에서 실행 가능한 정보 암호화 방법에 있어서,

정보 암호화를 위한 공개키와 암호개인키를 생성하는 단계와;

생성된 공개키와 암호화 실행 모듈을 무선 단말기로 전송하는 단계와;

무선 단말기에서 상기 공개키와 암호화 실행 모듈이 실행되어 암호화된 정보를 상기 게이트웨이를 통해 무선 단말기로부터 수신하는 단계와;

상기 암호개인키를 추출하여 수신한 암호화된 정보를 복호화하는 단계;를 포함하는 것을 특징으로 하는 정보 암호화 방법.

【청구항 7】

청구항 6에 있어서, 상기 암호화된 정보를 복호화 하는 단계는;

상기 암호개인키를 호출하여 상기 암호화된 정보에 포함된 암호화 압축키를 우선 복호화하는 단계와;

복호화된 상기 암호화 압축키로 상기 암호화된 정보에 포함된 전송 원문과 메시지 축약문을 압축 해제하는 단계와;

압축 해제된 상기 전송원문을 다시 메시지 축약하는 단계와;

메시지 축약된 전송 원문과 압축 해제된 메시지 축약문을 비교하여 동일하면 상기 암호개인키로 압축 해제된 전송 원문을 복호화하는 단계;를 포함함을 특징으로 하는 정보 암호화 방법.

【청구항 8】

네트워크를 통해 암호화 서버로부터 공개키와 같이 다운로드되어 유,무선 클라이언트 단말기에서 실행 가능한 정보 암호화 방법에 있어서,

클라이언트에 의해 입력된 정보를 상기 공개키로 암호화하여 전송 원문을 생성하는 단계와;

상기 암호화된 전송 원문을 메시지 축약하는 단계와;

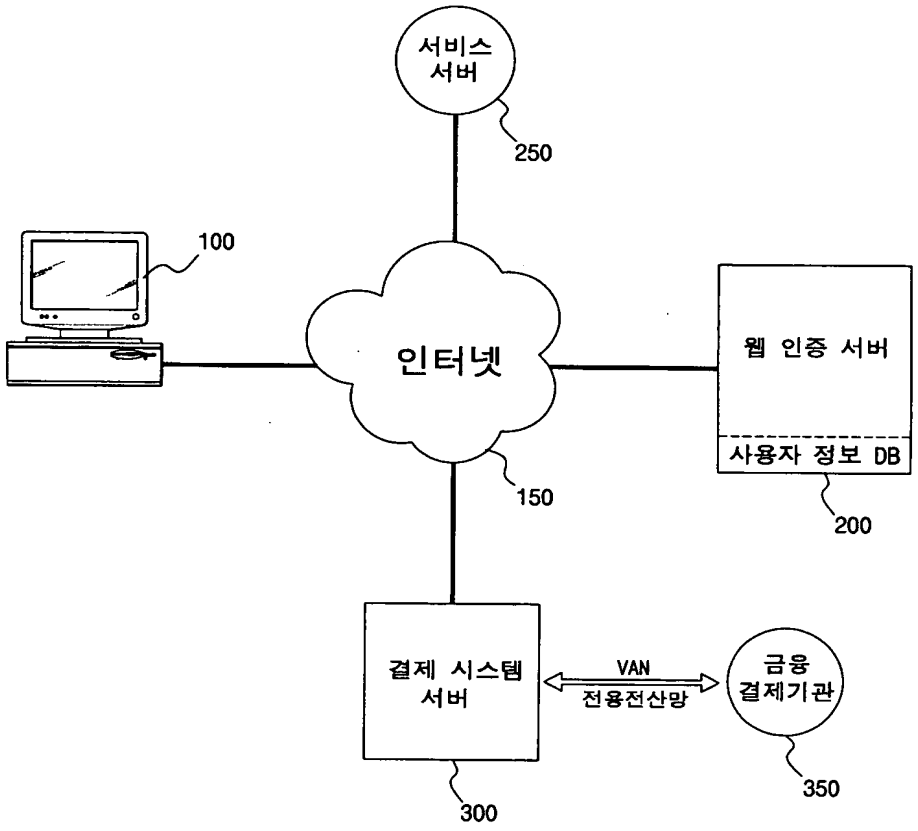
상기 공개키중 일부를 랜덤 추출하여 이루어지는 암호화 압축키를 이용하여 상기 전송 원문과 메시지 축약문을 압축하는 단계와;

상기 전송 원문을 암호화하는데 이용한 공개키로 상기 암호화 압축키를 암호화하는 단계와;

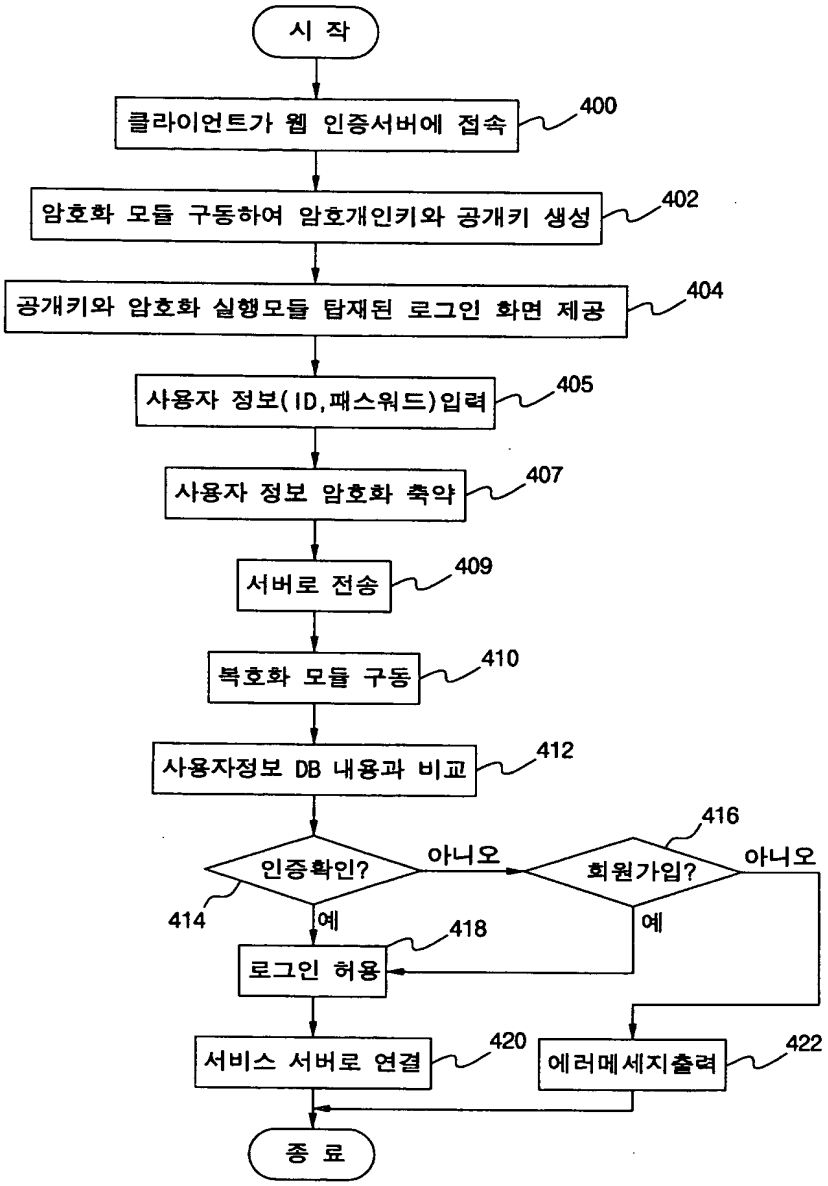
압축된 상기 전송 원문과 메시지 축약문 및 암호화된 암호화 압축키를 웹 문서 파일로 반환하여 전송하는 단계;를 포함함을 특징으로 하는 정보 암호화 방법.

【도면】

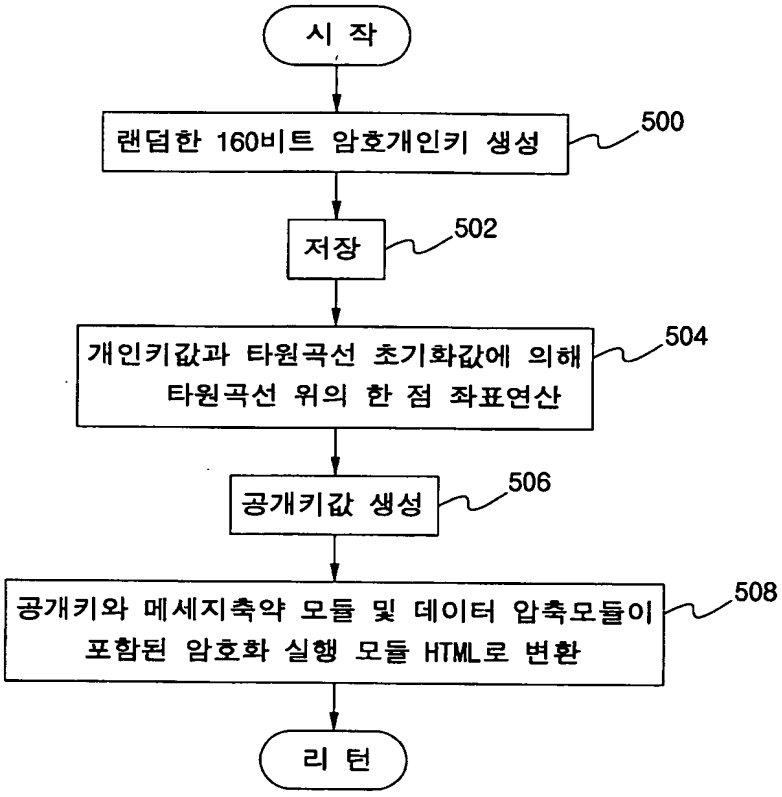
【도 1】


서비스 서버
250
100
인터넷
웹 인증 서버
사용자 정보 DB
150
200
결제 시스템 서버
VAN
전용전산망
금융 결제기관
300
350

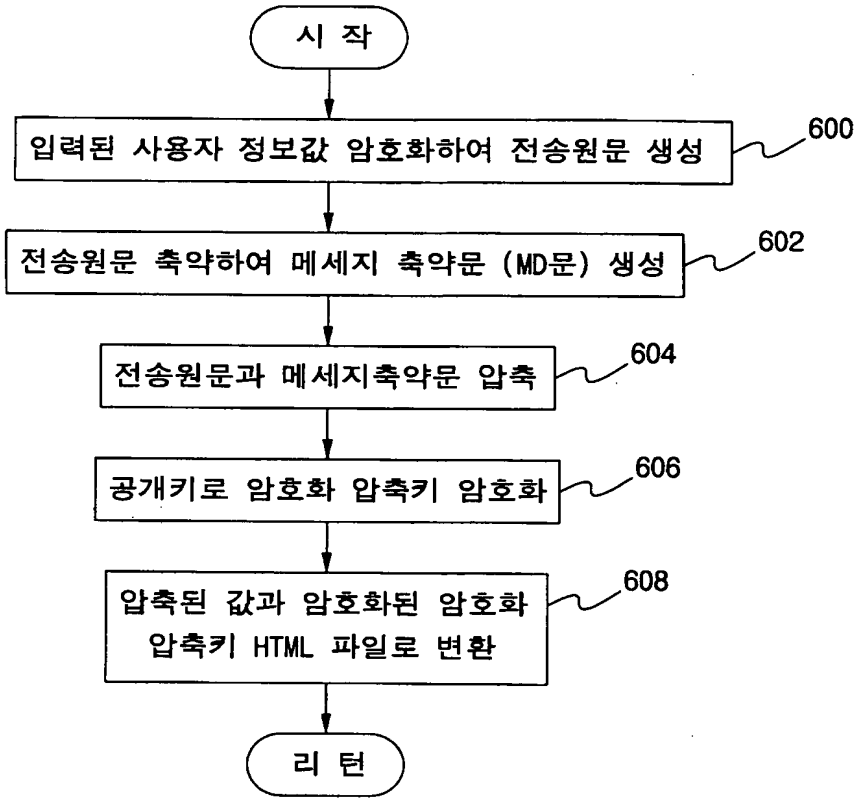
【도 2】


시 작
클라이언트가 웹 인증서버에 접속
400
암호화 모듈 구동하여 암호개인키와 공개키 생성
402
공개키와 암호화 실행모듈 탑재된 로그인 화면 제공
404
사용자 정보(ID,패스워드)입력
405
사용자 정보 암호화 축약
407
서버로 전송
409
복호화 모듈 구동
410
사용자정보 DB 내용과 비교
412
인증확인?
아니오
414
예
회원가입?
416
아니오
예
로그인 허용
418
서비스 서버로 연결
420
에러메세지출력
422
종 료

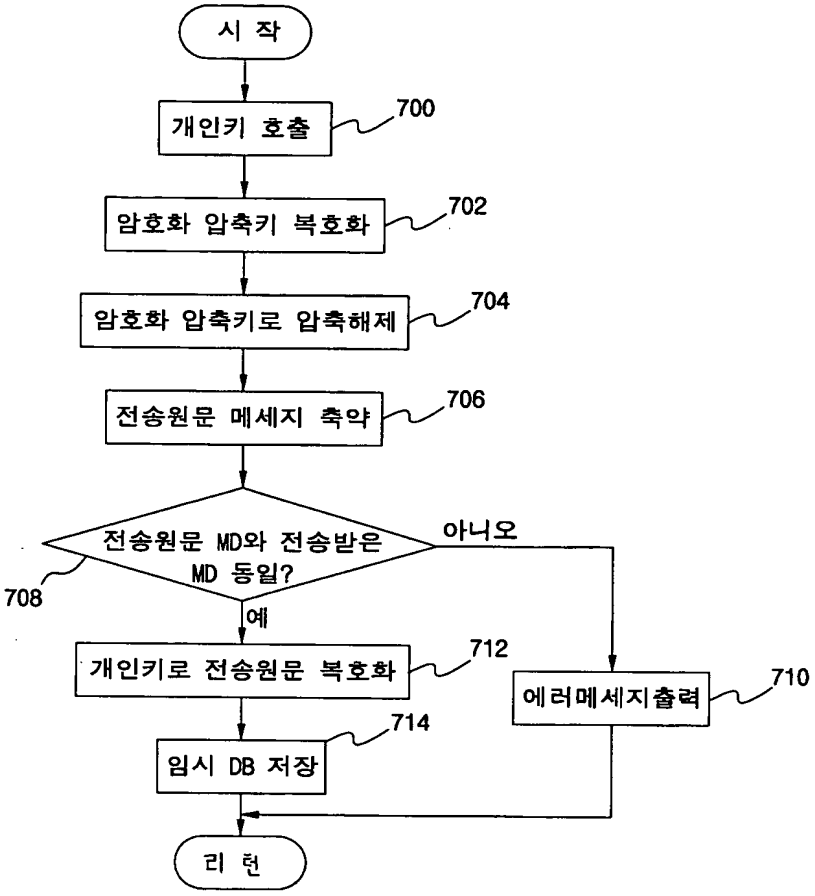
【도 3】


시 작
랜덤한 160비트 암호개인키 생성
500
저장
502
개인키값과 타원곡선 초기화값에 의해
타원곡선 위의 한 점 좌표연산
504
공개키값 생성
506
공개키와 메세지축약 모듈 및 데이터 압축모듈이
포함된 암호화 실행 모듈 HTML로 변환
508
리 턴

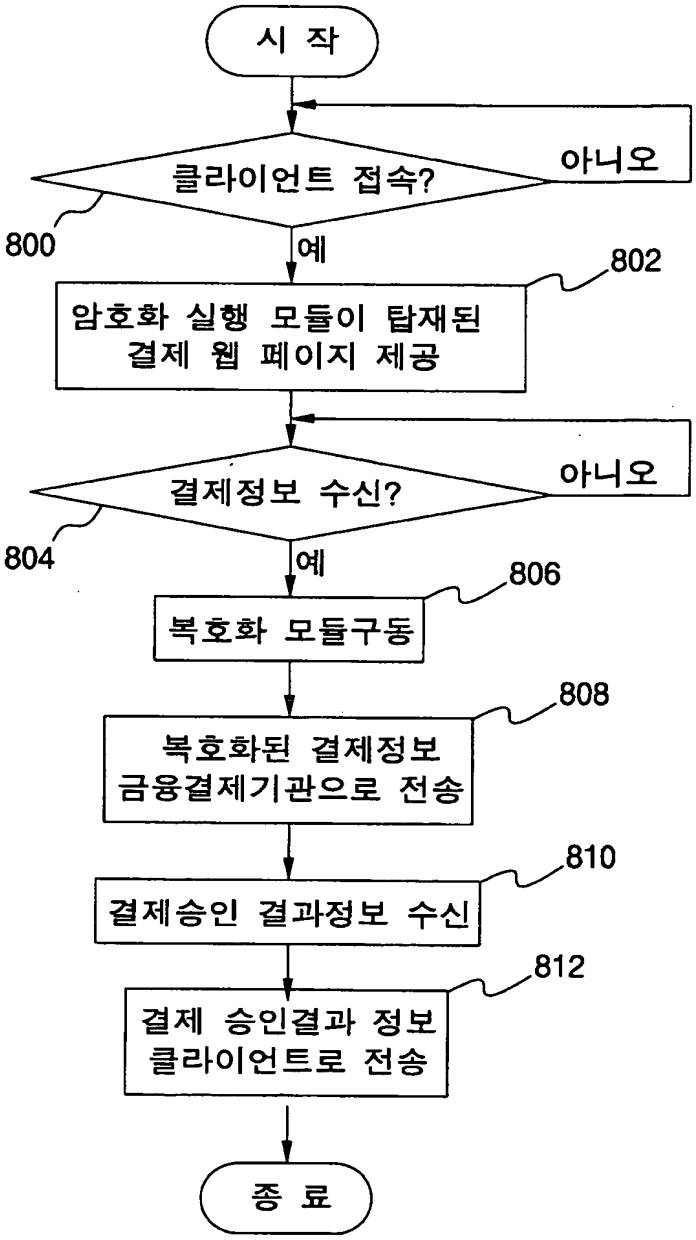
【도 4】


시 작
입력된 사용자 정보값 암호화하여 전송원문 생성
600
전송원문 축약하여 메세지 축약문 (MD문) 생성
602
전송원문과 메세지축약문 압축
604
공개키로 암호화 압축키 암호화
606
압축된 값과 암호화된 암호화 압축키 HTML 파일로 변환
608
리 턴

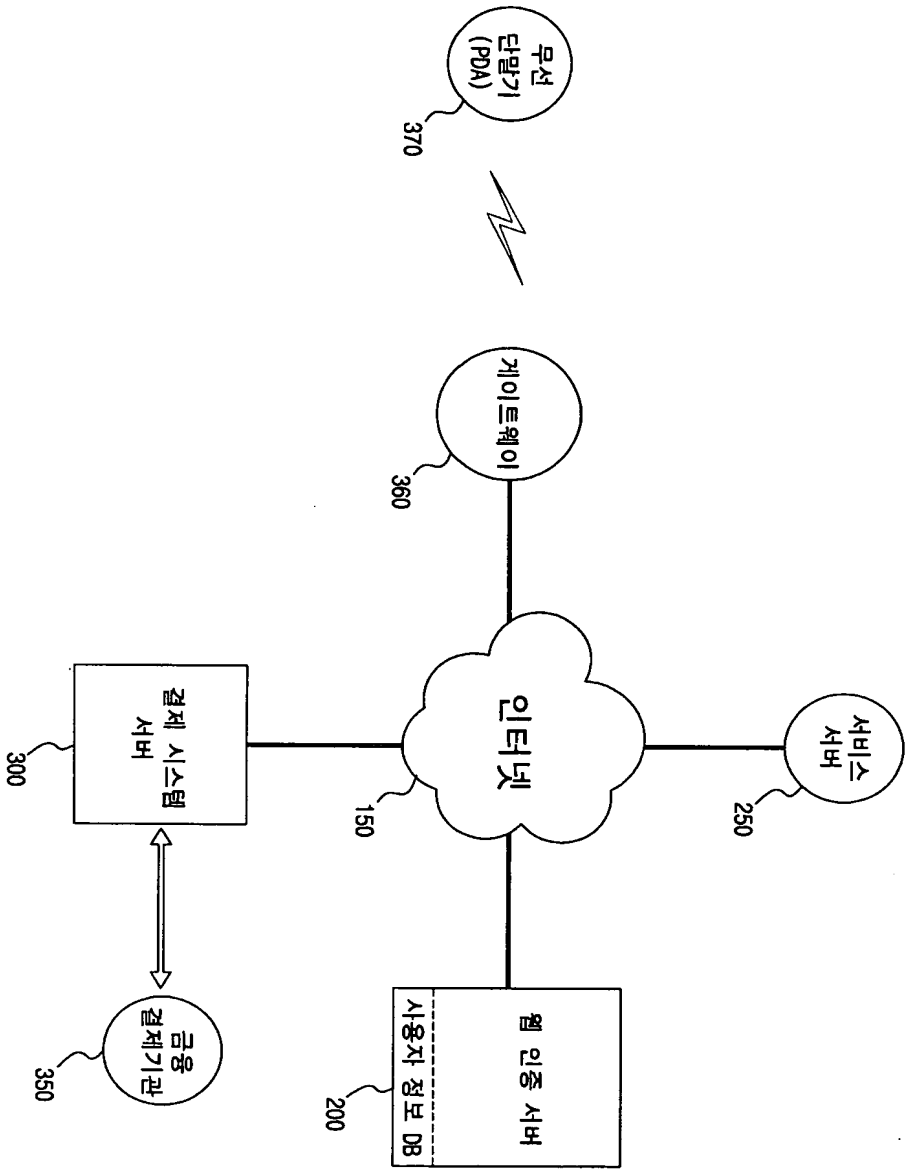
【도 5】


시 작
개인키 호출
700
암호화 압축키 복호화
702
암호화 압축키로 압축해제
704
전송원문 메세지 축약
706
전송원문 MD와 전송받은 MD 동일?
708
아니오
예
개인키로 전송원문 복호화
712
에러메세지출력
710
임시 DB 저장
714
리 턴

【도 6】


시 작
클라이언트 접속?
아니오
800
예
802
암호화 실행 모듈이 탑재된
결제 웹 페이지 제공
결제정보 수신?
아니오
804
예
806
복호화 모듈구동
808
복호화된 결제정보
금융결제기관으로 전송
810
결제승인 결과정보 수신
812
결제 승인결과 정보
클라이언트로 전송
종 료

【도 7】


무선 단말기 (PDA)
370
게이트웨이
360
인터넷
150
결제 시스템 서버
300
서비스 서버
250
금융 결제기관
350
웹 인증 서버
사용자 정보 DB
200